The claims defining the invention are as follows:

1. A method of establishing secure data transmission in a communications network between a client and a remote network entity, the method comprising the steps of:

(a) encoding an optical media security token with encrypted information, and

(b) using the encrypted information to establish said secure data transmission.

2. A method according to claim 1, wherein the encrypted information includes token and user identification information, step (b) including

(c) verifying at the client the authenticity of the token identification information,

(d) upon verification, transmitting the user identification information to the remote network entity,

(e) verifying at the remote network entity the authenticity of the user identification information, and

(f) verifying at the remote network entity the authorisation of the user to access one or more applications.

3. A method according to either one of claim 1 or 2, wherein the security token comprises optical media such as a CD-ROM, DVD or CD-MO.

4. A method according to any one of the preceding claims, wherein step (a) includes:

generating a first digital certificate including the token identification information, and

storing the first digital certificate on the security token.

5. A method according to claim 4, wherein step (c) includes:

decrypting the first digital certificate, and

comparing the token identification information with reference token identification data.

6. A method according to any one of the preceding claims, wherein step (a) includes:

generating a second digital certificate including the user identification information, and

storing the second digital certificate on the security token.

7. A method according to claim 6, wherein step (e) includes:

decrypting the second digital certificate by using the public key of a Certification Authority.

8. A method according to claim 7, wherein step (e) includes:

comparing the user identification information with a certificate revocation list maintained by the Certification Authority.

9. A method according to either of claims 7 or 8, wherein step (d) includes:

generating client data for transmission to the remote network entity,

attaching a user digital signature to the client data, and

transmitting the client data and user digital signature to the remote network entity.

10. A method according to claim 9, wherein step (e) includes:

using the decrypted second digital certificate to decrypt the client data at the remote network entity.

11. A method according to any one of the preceding claims, wherein step (f) includes:

sending a challenge value from the remote network entity to the client,

sending a response value from the client to the remote network entity,

comparing the challenge and response values at the remote network entity.

12. A method according to claim 11, and further including:

maintaining in a user profile database a user password,

wherein the response value is generated at the client by using the user password, a user private key and the challenge value.

13. A method according to claim 12 herein the challenge and response values are compared by using the user password, a user public key and the challenge value.

14 A method according to any one of the preceding claims, wherein step (c) is repeated up to a predetermined number of times to verify user authorisation.

15 15 A secure data transmission system comprising a client and a remote network entity interconnected by a communications network, the client being adapted to read an optical media security token bearing encrypted information.

16. A secure data transmission system according to claim 15, wherein the encrypted information includes token and user identification information, and wherein

the client includes a first data processing unit and associated first memory device for storing code to causing the client to verify the authenticity of the token identification information, and

upon verification, transmit the user identification information to the remote network entity, and wherein

the remote network entity includes a second data processing unit and associated second memory device for storing code to cause the remote network entity to verify the authenticity of the user identification information, and verify the authorisation of the user to access one or more applications.

17. A secure data transmission system according to claim 16, and wherein the code causes the client and/or the remote network entity to perform the steps of any one or more of claims 1 to 14.

18. A remote network entity for use with a secure data transmission system according to claim 16, the remote network entity including a second data processing unit and associated second memory device for storing code to cause the remote network entity to verify the authenticity of the user identification information, and verify the authorisation of the user to access one or more applications.

19. A client for use with a secure data transmission system according to claim 16, the client including a first data processing unit and associated first memory device for storing code to cause the client to verify the authenticity of the token identification information, and

upon verification, transmit the user identification information to the remote network entity.

20. A security token for use in a method according to any one claims 1 to 14, the optical media security token comprising optical media such as a CD-ROM, DVD or CD-MO.